National Information Assurance Acquisition Policy

This article reviews the national policy governing the acquisition of information assurance (IA) and IA-enabled information technology products and becomes effective July 1, 2002. The National Security Telecommunications and Information Systems Security Policy No. 11 was issued by the National Security Telecommunications and Information Systems Security Committee in January 2002.

The National Security Telecommunications and Information Systems Security Policy No. 11 (NSTIS-SP No. 11) was written to address the problems associated with acquiring commercial off-the-shelf (COTS) security and security-enabled information assurance (IA) products. While this policy includes helpful ideas and information to successfully complete the acquisition process, it is not a stand-alone document. Its origin can be tied back to Department of Defense (DoD) Information 5000.2-R. The current agency implementing this policy is Global Information Grid 6108510. There are also emerging policies awaiting DoD approval: directive 8500.aa and instruction 8500.bb.

Accordingly, the NSTIS-SP No. 11 has been developed as a means of addressing these problems for those products acquired for national security applications. The policy also rightfully points out that protection of systems encompasses more than just acquiring the right product. Once acquired, these products must be integrated properly and subject to an accreditation process, which will ensure total integrity of the information and systems to be protected.

The Policy

IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated and validated government-off-the-shelf (GOTS) or COTS IA and IA-enabled information technology (IT) products. These products should provide for the availability of the systems; ensure the integrity and confidentiality of information, and the authentication and non-repudiation of parties in electronic transactions.

Effective Jan. 1, 2001, preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) that have been evaluated and validated, as appropriate, in accordance with the following:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement.
- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program.
- The NIST Federal Information Processing Standard (FIPS) validation program.

The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

By July 1, 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified shall be limited only to those that have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the three sub-bullets.

The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information shall be limited to products that have been evaluated by the NSA, or in accordance with NSA-approved processes.

Normally, a complementary combination of IA/IA-enabled products is needed to provide a complete security solution to a given environment. Thus, in addition to employing validated IA/IA-enabled products, a solution security analysis should be conducted as part of the certification and accreditation process. In support of this, NSA shall provide guidance regarding the appropriate combinations and implementation of GOTS and COTS IA and IA-enabled products.

Subject to policy and guidance for non-national security systems, departments and agencies may wish to consider the acquisition and appropriate implementation of validated COTS IA and IA-enabled IT products. The use of these products may be appropriate for systems that process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems that may be associated with the operation and/or maintenance of critical infrastructures as defined in Presidential Decision Directive No. 63 (PDD-63), Critical Infrastructure Protection.

Responsibilities

Heads of U.S. departments and agencies are responsible for ensuring compliance with the requirements of this policy.

Exemptions and Waivers

COTS or GOTS IA and IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirements of this policy. Information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions considered as replacement upgrades at the earliest opportunity.

Waivers to this policy may be granted by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) on a case-by-case basis. Requests for waivers, including a justification and explanatory details, shall be forwarded through the director, National Security Agency (DIRNSA), ATTN: V1, who shall provide appropriate recommendations for NSTISSC consideration. Where time and circumstances may not allow for the full review and approval of the NSTISSC membership, the chairman of the NSTISSC is authorized to approve waivers to this policy, which may be necessary to support U.S. government operations that are time-sensitive, or where U.S. lives may be at risk.

For additional information or clarification, contact the National Security Agency at (410) 854-6805, or toll free at 1 (888) NSTISSC, or e-mail <nstissc@radium. ncsc.mil>.◆